VMware vCloud Air
Basic Technical Questions

VMware vCloud® Air™ Overview

Q. We don't have VMware vCloud Director®. Can we still use this service?

A. Absolutely. The key benefit of the hybrid cloud is to augment your VMware vSphere® resources with compatible and scalable cloud infrastructure. You may even use this service independently of your private data center should you choose.

Q. What are the change/maintenance windows for the service?

A. VMware vCloud Air leverages vSphere vMotion® so that scheduled maintenance windows should rarely, if ever, interrupt workloads running on the service. If scheduled maintenance is required we will make every effort to inform our customers a minimum of 24 hours in advance.

Q. Is there any need for someone on our team to physically visit the data center?

A. No. Our data center is managed by a highly focused team of experts and adheres to strict security practices. Customers are not permitted within the confines of the data center itself without executive sponsorship. This is for the security of all our customers.

Q. What industry regulations and security certifications has VMware vCloud Air been audited against?

A. At this time, VMware vCloud Air has achieved ISO/IEC 27001 certification of its Information Security Management System and completed its SSAE 16 SOC 1 Type II and SOC 2 Type II examinations under the previous service name, VMware vCloud® Hybrid Service™. vCloud Air has also completed an independent examination against applicable controls of HIPAA/HITECH. These audits and examinations are all being completed by Brightline CPAs and Associates – an ANAB accredited certification body. For more information about security and/or compliance, please refer to the Security FAQ.

Compute Services:

Q. What resources are being provided with this service?

A. A **Dedicated Cloud** begins with 30GHz of Compute (vCPU) capacity, 120GB of vRAM, and 6TB of Storage. Also included are 3 public IP addresses, as well as a 50Mbps network link, burstable to 1Gbps.

A **Virtual Private Cloud** begins with 5GHz of Compute (vCPU) capacity, 20GB of vRAM, and 2TB of Storage. Also included are 2 public IP addresses, as well as a 10Mbps network link, burstable to 50Mbps.

Q. Are resources shared with other customers?

A. **Dedicated Cloud** customers are provided physically isolated pools of vCPU and vRAM. Compute nodes within our data centers for Dedicated Cloud are "air-gapped". Network and Storage are logically isolated on modern, high-end multi-tenant infrastructure, with appropriate resource guarantees in place. Dedicated Cloud customers are also provided a segregated cloud management stack, unique to their service and not shared with other customers.

Virtual Private Cloud customers are provided pools of vCPU, vRAM, Network and Storage using the same design architecture as Dedicated Cloud, but are logically isolated. Based on vSphere resource isolation, physical resources are operating in a multi-tenant design, but tenants are provided strict guarantees to their share of resources, and load is evenly balanced across the infrastructure, ensuring robust and scalable availability to everyone in the cloud.

Q. What hardware is being provided with this service?

A. VMware vCloud Air provides secure, robust and scalable x86-based infrastructure, designed for compatibility with your vSphere data center. Each vCloud Air offering is architected for the cloud using the best-in-class hardware available. To stay on the leading edge of the cloud technology movement, our specific hardware vendors remain subject to change and are not disclosed.

Q. What types of workloads are suitable for this Cloud?

A. vCloud Air is a production-ready environment capable of running the most demanding mission-critical workloads, with the control and agility to accommodate workloads of all kinds.

vmware®

Q. What sort of usage reporting or consumption dashboard is provided?

A. The vCloud Air dashboard provides an aggregate view of the allocation of cloud resources across Virtual Data Centers. Along with viewing the utilization of cloud capacity within each Virtual Data Center, virtual machine-level monitoring of CPU and memory usage, disk reads, and disk writes is available directly from the portal. Third-party partner tools using in-guest agents can also be used to monitor capacity and usage.

Q. Can we use our own management software or other tools to monitor our environment?

A. Yes. While customers do not have the ability to monitor the management stack directly, users are able to use any technology that leverages the vCloud API such as VMware vCloud® Automation Center™, vCenter™ and vCenter Orchestrator™. A vCenter Operations Management Pack for vCloud Air is available to get operational visibility of both on-premises and vCloud Hybrid Service resources from a single vCenter Operations Manager™ console. Customers may also deploy agent-based tools, such as HypericHQ, to report back to the local data center.

Q. What UI or API access is provided?

A. To operate and consume vCloud Air, customers are provided access to a Unified Service Dashboard. Customers are also provided access to the vCloud Director 'tenant' UI. Finally, we provide access to the vCloud API with vCloud Air extensions for integrating vCloud-aware applications and platforms such as vCloud Automation Center.

Q. How does VMware guarantee the availability and redundancy of the vCloud Air environment?

A. vCloud Air is delivered using infrastructure that is architected for High Availability, leveraging vSphere vMotion, Distributed Resource Scheduler™ (DRS), and vSphere HA to migrate live workloads and/or automatically restart VMs in the event of unexpected issues. The Edge Gateways are also highly available in an active-standby pair to ensure that networks are protected and available after an event.

Q. For applications in the cloud that contain highly sensitive data, how will that data be protected from others?

A. The vSphere and vCloud platform, by design, provides exceptional levels of resource isolation, ensuring that deployed applications are unable to be accessed by unauthorized users. Users also play a key role in security, and customers are encouraged to adopt or bring their own encryption and security practices where appropriate. Further, customers are provided user-level access control, mandatory HTTPS connection to the portal, IPsec VPN tunneling, and tremendous amounts of physical security procedures within the physical data center itself.

Storage and Networking Services:

Q. What type of storage comes with the service?

A. There are two tiers of persistent, block-level storage in vCloud Air:

- SSD-Accelerated Tier for the most demanding applications
- Standard Storage Tier for the most cost-efficient solution

Workloads can be moved between storage tiers and a single virtual machine can be attached to disks of different tiers.

Q. Are there any bandwidth or traffic limits/restrictions?

A. The **Dedicated Cloud** service includes 50Mbps of guaranteed bandwidth, burstable to 1Gbps.

The **Virtual Private Cloud** service includes 10Mbps of guaranteed bandwidth, burstable to 50Mbps.

Additional bandwidth is available through Direct Connect ports.

Q. Can we use VPN tunnels to connect to this service?

A. Yes. The service supports creating IPsec VPN tunnels using the Edge Gateway service to any IPsec VPN device. There are several options for self-service deployment of VPN tunnels between: Networks within the same Virtual Data Center; Networks in different Virtual Data Centers (Dedicated Cloud Only); as well as networks in your local data center using either software or hardware VPN solutions.

Establishing IPsec VPN connections is a self-service feature, but our vCloud Air Global Support team is standing by to offer assistance when required.

Q. How do we bring data and workloads from our other environments/data centers?

A. We provide multiple ways of migrating your workloads:

- Use vCloud Connector® to transfer workloads from your on-premises vSphere or vCloud environment to your vCloud Air environment.
- Offline Data Transfer can also be used to migrate very large data sets into your vCloud Air environment using an external storage device. This is available as a paid, per-use service from VMware.
- vCloud Director also provides customers with the capability to import or export OVF Virtual Machine images, or other media.

Q. What is VMware vCloud Air Direct Connect?

A. Direct Connect is a private, high-throughput, dedicated connectivity option available with vCloud Air, in addition to a standard IPsec VPN connection. VMware works with leading telco providers to establish these high-throughput and secure links from customer data centers (either in a remote location or in the same co-location facility) to vCloud Air Dedicated Cloud or Virtual Private Cloud instances.

There are two parts to the Direct Connect service:

1. Customer side connection: The telco partner manages the connection from customer's onsite data center (or co-location cage) to the telco partner's switch. The partner handles provisioning and order management of this connection.
2. vCloud Air side connection: VMware provides a port connection from the telco partner's switch to customer's Edge Gateway in vCloud Air. VMware manages provisioning and order management of this connection.

More information is available on the Direct Connect data sheet

Q. What are the differences between standard vCloud Air connection and Direct Connect?

A. The standard vCloud Air connection is routed over the Internet whereas vCloud Air Direct Connect is a dedicated secure private link. The key differences are highlighted below:

	STANDARD CONNECTION	DIRECT CONNECT
Speed	Dedicated Cloud: Up to 1Gbps Virtual Private Cloud: Up to 1Gbps	Dedicated Cloud: Up to 10Gbps Virtual Private Cloud: Up to 1Gbps
Connection Type	Routed over Internet	Dedicated link
Secure Connection	Via IPsec VPN	Private by default
Single or Multi-Point	IPsec is point-to-point	Point-to-point or multi-point (Varies by telco partner)
Pricing	Included in Core: Dedicated Cloud: 50Mbps Virtual Private Cloud: 10Mbps	Monthly port connection fee Additional circuit fees vary by telco partner

Availability Services: Data Protection

Q. What is vCloud Air Data Protection?

A. Data Protection is an optional data backup and recovery solution for Dedicated Cloud and Virtual Private Cloud instances. Data Protection is an agent-less, self-service, policy-driven backup recovery service with image-level backups to ensure all operating system, file system and application data residing within a virtual machine are captured as a snapshot before committed to backup media.

Q. What backup policy options are available?

A. Policies can be defined for a single virtual machine (in the form of a vApp) or for an entire Virtual Data Center. Each protected item can set a different data retention policy of up to 365 days with selectable backup start times. Backup of a vApp can also be manually started in the vCloud Air UI.

Q. What recovery options are available?

A. Recovery from backup can be from any available recovery point. Recovering from a backup can either replace the protected virtual machine (in-place restore) or be deployed as a separate virtual machine (out-of-place restore).

Q. Do the backups consume storage from my cloud instance?

A. No. The storage used by Data Protection is specifically assigned to the Data Protection offering. Backups will never consume storage from your cloud instance.

Q. Does each backup consume the same amount of storage every time?

A. Data Protection leverages synthetic full backups with change block tracking to backup Virtual Machines (vApp or VDC level). The initial backup is a full backup, but subsequent backups only capture the daily unique changes, saving on storage consumption.

Q. How long does it take to restore a vApp or virtual machine?

A. The recovery period depends on the size of the virtual machine and the storage tier. For example, a 40GB virtual machine being restored to SSD-Accelerated storage would complete sooner than a 200GB virtual machine being restored to Standard Storage.

Availability Services: Disaster Recovery

Q. What is vCloud Air Disaster Recovery?

A. vCloud Air Disaster Recovery is a disaster recovery service that allows customers to increase business resiliency while protecting applications with minimal investment. The service ensures operational consistency with realizable cost and resource savings while providing a failover environment for dependable recovery in the event of a disaster. Additional information can be found in the Disaster Recovery FAQ

Q. What are the minimum requirements to take advantage of vCloud Air Disaster Recovery?

A. The requirements in the primary data center include:

- vSphere 5.1 or above, Essentials Plus or higher (including Standard, Enterprise, Enterprise Plus)
- vCenter 5.1 or above
- vSphere Replication Appliance 5.6
- Public internet connectivity

In addition, an active vCloud Air Disaster Recovery subscription with Virtual Infrastructure administration rights is needed.

Q. What is the primary method of backup being used?

A. vCloud Air Disaster Recovery takes advantage of VMware vSphere Replication™ technology – a hypervisor-based replication solution that operates at the individual virtual machine disk (VMDK) level, allowing replication from any storage type. Changed blocks in the virtual machine disk at the primary site are sent to vCloud Air in a non-intrusive manner, requiring no change to the virtual machine configuration or management.

Q. Is quiescing for SQL or other applications supported?

A. Yes, vSphere Replication supports quiescing with Microsoft Volume Shadow Services (VSS). If an application is VSS- aware, you can select "Quiescing via VSS" in the configuration of replication.

Q. Can replications be seeded offline?

A. Yes – replication seeds through vCloud Connector or OVF exports are supported. For an additional fee, initial replication can also be seeded with Offline Data Transfer where a physical NAS device is shipped to you. You place a seed copy of the protected virtual machines and ship it back to VMware where we will copy it into your environment (shipping costs all included).

Q. How secure are replications? Is this data traveling across the Internet?

A. Yes, replication traffic takes place over the Internet. To secure this traffic, the vSphere Replication appliance now includes an encryption module for point-to-point encryption to vCloud Air without the need for a separate VPN tunnel.

Q. What networking options are available within the Disaster Recovery environment?

A. A Disaster Recovery environment in vCloud Air has the same networking capabilities as the standard Virtual Private Cloud. That means there is one Edge Gateway available for each environment, which can be used to create up to 9 different, isolated or routed networks. The Edge Gateway can also be configured with NAT and firewall rules, DHCP or static IP assignments, and it can also be used to set up VPN and load balancing. During the configuration of replication, a virtual machine will be attached to one of the available networks.

Q. What is maximum scalability of Disaster Recovery?

A. At this time, there is a limit of 500 virtual machines per Disaster Recovery environment. This is because there is a 1-to-1 mapping of vCenter to each Disaster Recovery environment and there is currently a limitation of 500 virtual machines per vSphere Replication appliance, per vCenter. This also means that a vCenter environment designated for replication to vCloud Air cannot also simultaneously map to replication in another data center.

Q. What are the automation options for failover?

A. As Disaster Recovery is a self-service offering, it does not currently include a run book solution. Automation options for failover include the use of the vCloud APIs in conjunction with tools like vCenter Orchestrator, vCloud Automation Center, Puppet, etc. Failback is a manual operation at the moment.

Q. How do I initiate a test failover?

A. First contact Global Support Services (GSS) to enable the test failover and you will have 7 days to perform your tests. When you have completed your tests, initiate a test cleanup process to return the virtual machines in vCloud Air to the standby state.

Q. How do I "declare" a disaster?

A. There is no official need to notify anyone to "declare" a disaster and fail over your machines. You can simply invoke the failover process from vCenter, vCloud Air UI, or through an API call. VMware will ensure that the resources you have subscribed to will be available to then start bringing your machines online. You can then start your run book process to bring your applications online.